Security

January 2005

Essential Practices for Information Technology Examination Manual
IT Section

FCA Essential Practices for Information Technology

Based on Industry Standards and FFIEC Examination Guidance

Table of Contents

Page

Security

Introduction:

Information is an important business asset and, like other important assets, must be protected. To conduct ongoing operations, the institution must have accurate information (or data) available when needed. If this information is also sensitive, such as a customer's financial records or an employee's personnel files, it must be protected to preserve the individual's privacy and to protect and safeguard the institution's reputation and legal responsibilities.

Information security is the process by which an institution protects and secures systems, media, and facilities that process and maintain information. Key elements of any security program must address:

- **Confidentiality**—the assurance that information is accessible only to those authorized to have access;
- **Integrity**—the assurance that information and processing methods are accurate and complete; and
- **Availability**—the assurance that authorized users have access to information and associated assets when needed.

These concepts are achieved by implementing controls, which include policies, procedures, practices, organizational structures, and software applications. These controls must be established to ensure security is commensurate with the institution's size, risk, and operational complexity. The Essential Practice Statements below are baseline expectations. As the institution evolves, additional security measures may be necessary.

Security is an ongoing process that is the responsibility of everyone within the institution. This responsibility begins with the board of directors (board), which establishes necessary security policies, culture, and direction. Management must implement the board's direction through procedures, internal controls, and training. Board policy and management processes must provide strong support and commitment to security programs and practices because the board and senior management's attitude towards security affects the entire institution's commitment to security. Expectations related to board policy and management guidance are discussed in more detail in *The Director's Role* and the ***Management*** and ***Information Technology Management*** sections of the *FCA Examination Manual*.

Examination Objectives:

Determine if the board and management have established and maintained effective security over the institution's facilities, systems, and media that process and store vital information for business operations. This is accomplished through the following examination objectives:

- **Risk Assessment**—Evaluate the adequacy of the institution's risk assessment process for information security. Key elements of this process may include management's self-assessment of the IT environment (threats, vulnerabilities, and compensating controls).
- **Risk Management**—Evaluate the risk management process used to identify, control, and mitigate security risks.
- **Board and Management Oversight**—Assess the adequacy of information security oversight by examining security policies, procedures, plans, and controls. Oversight responsibilities also extend to all outsourced services and contractors.
- **Internal Controls**—Evaluate the effectiveness of preventive and detective controls designed to identify material deficiencies on a timely basis.

Examination Procedures:

Examination activities should be based on the operational complexity and use of information technology. The examination should begin with a review of audit activities and the risk assessment for information security. If a service provider performs information processing for the institution, then the institution's management must perform sufficient due diligence to ensure appropriate internal controls and sound business practices are maintained. At a minimum, the ***Essential Practices*** for Security should be clearly documented and functioning within the internal control environment. More in-depth examination procedures (such as those found in the *FFIEC Information Security Booklet*) should be evaluated and incorporated into the examination scope as an institution's size, risk, and complexity increases.

Security

Element		
Essential Practices Statement	**Industry Standard Reference**	**FFIEC IT Examination Handbook Reference**
1. General Security		
Security Officer		
Appoint a security officer to be responsible for implementing, monitoring, and enforcing the security rules that management has established and authorized (consistent with board policies). ***Reason:*** *A designated security officer provides the institution with a central point to coordinate management's security administration, ensure consistency across the institution, and assist in security-related decision making.*	ISO/IEC 17799:2000, Section 4.1.5, "Specialist Information Security Advice."	Information Security Booklet (Dec. 2002), p. 5.
Security Plan		
Based on a defined data classification system, document an institution-wide security plan which includes: • **Physical security** • **Logical security** • **Backup processes and business continuity planning** • **Employee training and awareness program** ***Reason:*** *The institution needs a comprehensive written security plan to minimize exposure to all threats and risks. Security is the responsibility of every employee within the institution, not just those working in IT-related departments. Institution-wide security awareness training puts emphasis on institution-wide security responsibilities.*	ISO/IEC 17799:2000, Section 3.1, "Information Security Policy"; Section 5.2, "Information Classification"; Section 6.2.1, "Information Security Education and Training."	Information Security Booklet (Dec. 2002), pp. 7-14. FedLine Booklet (Aug. 2003), p. 4.
User Training		
Implement a user education program to promote employees' awareness of information security threats and concerns and their obligation to challenge any person or procedure that may violate security systems. Ensure employees are aware of procedures for reporting observed or suspected security weaknesses and incidents. ***Reason:*** *To minimize possible security risks, all users should be aware of the institution's security policies and the repercussions of violating them. Security incidents should be reported through appropriate management channels as quickly as possible. Training materials would typically review the acceptable use policy and include issues like log-on requirements, password*	ISO/IEC 17799:2000, Section 6.2 "User Training"; Section 6.3.1 "Reporting Security Incidents"; Section 6.3.2 "Reporting Security Weaknesses."	Information Security Booklet (Dec. 2002), p. 62. E-Banking Booklet (Aug. 2003), p. 30.

Security

Element	Essential Practices Statement	Industry Standard Reference	FFIEC IT Examination Handbook Reference
	administration guidelines, etc. Training should also address social engineering, and the policies and procedures that protect against social engineering attacks. Many institutions implement a signed security awareness agreement along with periodic training and refresher courses.		
2. Physical Security			
	Foundation: Effective security at an institution begins with strong physical security measures. Physical security refers to the various measures or controls that protect the confidentiality, integrity, and availability of information and systems from threats of theft, fire, flood, malicious destruction, mechanical failure, or power failure. Management can establish physical security by creating physical barriers around the business premises and information processing areas. Examples of physical barriers are walls, locked (electronic or conventional) entry gates, or staffed reception and guard desks. Adequate physical security is necessary to prevent, detect, minimize, and recover losses from damage or unauthorized use of equipment, software, or data. Security measures must protect against both intentional and accidental threats and should be commensurate with the identified risks.	ISO/IEC 17799:2000, Section 7, "Physical and Environmental Security."	Information Security Booklet (Dec. 2002), pp. 44-48.
Building			
	Physically secure or monitor (i.e., security guard, receptionist) entrances to the building. ***Reason***: *Appropriate security barriers and entry controls (key pads, key card systems, biometrics, tokens, etc.) prevent unauthorized access, damage, theft, and interference to business premises and information.*	ISO/IEC 17799:2000, Section 7.1.1, "Physical Security Perimeter."	Information Security Booklet (Dec. 2002), p. 45.
Equipment			
	Physically protect equipment from security threats and environmental hazards. ***Reason:*** *Protection of equipment (including that used offsite) is necessary to reduce the risk of unauthorized access to data and to protect against loss or damage. Such protection should also consider equipment siting (location) and ultimate disposal or destruction [Refer to **Operations**—Equipment Removal/Data Destruction].*	ISO/IEC 17799:2000, Section 7.2, "Equipment Security."	Information Security Booklet (Dec. 2002), pp. 44-48. E-Banking Booklet (Aug. 2003), pp. 29-30. FedLine Booklet (Aug. 2003), p. 5.

Security

Element		
Essential Practices Statement	**Industry Standard Reference**	**FFIEC IT Examination Handbook Reference**
Data Center (i.e., the computer room, the server room)		
Restrict access to the data center and other critical devices (servers, terminals, etc.) to authorized personnel. Key controls include: • **Locked data center** • **Escorting unauthorized personnel** • **Unidentified location** ***Reason:*** *As noted previously, appropriate security barriers and entry controls prevent unauthorized access, damage, and interference to business premises and information. Restricting physical access to authorized personnel ensures that only those staff members whose job functions require the use of the information or equipment have access to it. Removing or limiting signage on doors to sensitive areas reduces the chance that an intruder or an unauthorized staff member could locate the equipment and damage it.*	ISO/IEC 17799:2000, Section 7.1.2, "Physical Entry Controls"; Section 7.1.3, "Securing Offices, Rooms, and Facilities."	Information Security Booklet (Dec. 2002), pp. 45-46.
• **Location**		
Strategically locate the data center in an area of the building that is safe from exposure to fire, flood, explosion, or similar hazards. ***Reason:*** *The data center houses the institution's most important information systems components (hardware, software, and data); therefore, it must be as safe as possible from hazards.*	ISO/IEC 17799:2000, Section 7.1.3, "Securing Offices, Rooms, and Facilities."	Information Security Booklet (Dec. 2002), p. 45.
• **Environmental Controls**		
Establish environmental controls for the data center, including: • **Sufficient air conditioning and humidity control systems to maintain temperatures within manufacturers' specifications.** • **Adequate fire detection and suppression systems or equipment (i.e., dry chemical, gas, or sprinklers).** • **Strategically located fire extinguishers. This equipment should be located throughout the building—not just the data center—and inspected at least annually.** • **An uninterruptible power supply (UPS) to continue operations during minor power fluctuations or enable the safe shut down of equipment during a prolonged power outage.**	ISO/IEC 17799:2000, Section 7.2.1, "Equipment Siting and Protection"; Section 7.2.2, "Power Supplies."	Information Security Booklet (Dec. 2002), pp. 45-46. Operations Booklet (Jun. 2004), pp. 17-21.

Security

Element		
Essential Practices Statement	**Industry Standard Reference**	**FFIEC IT Examination Handbook Reference**
• **Protection for equipment from the effects of static electricity and electrical surges.** ***Reason:*** *It is necessary to protect equipment to enable it to function properly and to safeguard it from loss or damage.*		
Cabling and Wireless Access Points		
Physically secure the building's network wiring infrastructure to prevent unauthorized access. This infrastructure may include wiring closet(s), cabling, and wireless access points. ***Reason:*** *Power and telecommunications connections that carry data or support information services must be protected from interception or damage.*	ISO/IEC 17799:2000, Section 7.2.3, "Cabling Security."	Information Security Booklet (Dec. 2002), pp. 46-48. E-Banking Booklet (Aug. 2003), p. 12; Appendix E, E-2. Operations Booklet (Jun. 2004), p. 18.
Data		
Protect data from fire, theft, destruction, alteration, and other physical hazards. ***Reason:*** *Data security controls are necessary to protect data and software resources from accidental or intentional disclosure to unauthorized persons or from unauthorized modification or destruction.*	ISO/IEC 17799:2000, Section 7.1, "Secure Areas"; Section 7.3, "General Controls."	Information Security Booklet (Dec. 2002), pp. 44-48. FedLine Booklet (Aug. 2003), pp. 5-6. Operations Booklet (Jun. 2004), p. 27.
3. Logical Security		
Foundation: Effective security controls often combine physical security and logical security by first governing physical access to computer facilities or equipment, and then governing logical access to the data stored within the physical system. Logical security refers to the standards and procedures designed to protect data against accidental or intentional unauthorized disclosure, modification, or destruction. Data, or information, is a business asset and is of no use to the institution if it is incorrect or not available. Additionally, if the information were disclosed inappropriately, the institution could lose business, damage its reputation, and face criminal or legal liabilities. Proper security over a user's logical access to systems and data is necessary to prevent unauthorized users from gaining access to application and system resources. Examples of logical access controls include user identification (user ID), passwords, and restricting user privileges. Biometrics and tokens can add another level of authentication control to bolster	ISO/IEC 17799:2000, Section 9, "Access Control."	Information Security Booklet (Dec. 2002), pp. 15-44. FedLine Booklet (Aug. 2003), p. 8. Operations Booklet (Jun. 2004), pp. 22-23.

Security

Element		
Essential Practices Statement	**Industry Standard Reference**	**FFIEC IT Examination Handbook Reference**
logical security. Again, the level of security must be commensurate with the institution's size, risk, and complexity.		
Authentication		
Assign unique user IDs to each user, review user accounts periodically to ensure access remains appropriate, adjust access rights when users change jobs, and immediately remove access rights when users leave the institution. ***Reason:*** *A unique user ID links an individual to actions on the network system and provides a mechanism to identify responsibility. Added authentication controls are necessary when user access to privileged or sensitive systems and information increases.*	ISO/IEC 17799:2000, Section 9.2.1, "User Registration"; Section 9.2.4, "Review of User Access Rights"; Section 9.5.3, "User Identification and Authentication."	Information Security Booklet (Dec. 2002), p. 17-18. E-Banking Booklet (Aug. 2003), p. 30. FedLine Booklet (Aug. 2003), p. 8.
Password Standards		
Establish and enforce appropriate password standards that require all users to: • **Select a unique password and keep it confidential.** • **Choose a password that is easy for the user to remember, but difficult for an intruder to guess. Do not use words found in a dictionary (any language), the names of family members or sports teams, or other terms associated with the user or institution.** • **Ensure passwords are not displayed in any form (i.e., when entered on computer screen, printed within reports, or written on a piece of paper in the user's desk).** • **Select a password with at least eight characters that include a combination of upper and lower case letters, numbers, and special characters.** • **Use unique passwords for a minimum of twelve months before reusing passwords.** • **Change the password regularly (i.e., at least every 90 days for general users and more frequently for administrators and privileged users).** ***Reason:*** *Passwords are the most common authentication mechanism for validating the user's identity and establishing access rights to information systems and facilities. The strength of an individual's password, and thus the amount of security provided, relies on continued confidentiality, appropriate complexity, and adequate change frequency.*	ISO/IEC 17799:2000, Section 9.2.3, "User Password Management"; Section 9.3.1, "Password Use." NSA's (National Security Agency) "The 60 Minute Network Security Guide", version 1.2, July 2002, p.8.	Information Security Booklet (Dec. 2002), pp. 19-21. E-Banking Booklet (Aug. 2003), pp. 32-34.

Security

Element	Essential Practices Statement	Industry Standard Reference	FFIEC IT Examination Handbook Reference
Access Control			
	Limit user access for any particular system resource to the minimum required to perform the job function. ***Reason:*** *Access beyond the minimum required for work to be performed exposes the institution's systems and information to a loss of confidentiality, integrity, and availability.*	ISO/IEC 17799:2000, Section 9.1, "Business Requirement for Access Control"; Section 9.2.2, "Privilege Management"; Section 9.4.1, "Policy on Use of Network Services." NSA's "The 60 Minute Network Security Guide", version 1.2, July 2002, p. 9	Information Security Booklet (Dec. 2002), pp. 15-17. E-Banking Booklet (Aug. 2003), p. 27. FedLine Booklet (Aug. 2003), pp. 8-9. Operations Booklet (Jun. 2004), p. 22.
Web Server Security			
	Secure web servers and the network infrastructure that supports them. ***Reason:*** *The web server is the most targeted and attacked host on most institutions' network. Security threats to web servers generally result in one or more of the following outcomes:* • *Malicious entities, including foreign governments and terrorist institutions, may exploit software bugs in the web server, underlying operating system, or active content to gain unauthorized access to the web server. Examples of unauthorized access are gaining access to files or folders that were not meant to be publicly accessible or executing privileged commands and/or installing software on the web server.* • *Denial of service (DoS) attacks may be directed to the web server denying valid users an ability to use the web server for the duration of the attack.* • *Sensitive information on the web server may be distributed to unauthorized individuals.* • *Sensitive information that is not encrypted when transmitted between the web server and the browser may be intercepted by an unauthorized party and then stolen, modified, or disclosed.* • *Information on the web server may be changed for malicious purposes. Web site defacement is a commonly reported example of this threat.* • *Malicious entities may gain unauthorized access to the*	NIST (National Institute of Standards and Technology) Special Publication 800-44, "Guidelines on Securing Public Web Servers ES-2 and 3."	Information Security Booklet (Dec. 2003), p. 47. E-Banking Booklet (Aug. 2003), pp. 29-30.

Security

Element	Essential Practices Statement	Industry Standard Reference	FFIEC IT Examination Handbook Reference
	institution's computer network via a successful attack on the web server. • *Malicious entities may attack external institutions from a compromised web server, concealing their actual identities, and perhaps making the institution from which the attack was launched liable for damages.* • *The server may be used as a distribution point for illegally copied software, attack tools, or pornography, perhaps making the institution liable for damages.*		
4. Firewalls			
	Foundation: Firewalls are an essential security control for an institution with an Internet connection. A firewall is a device or collection of components (computers, routers, and software) that enforces a boundary between two or more networks. They are ideally situated to inspect and block traffic and coordinate activities with network intrusion detection systems. While firewalls provide a means of protection against malicious attacks, they should not be relied on as the only defense. Institutions should complement firewalls with strong security policies, management oversight, and other controls.	ISO/IEC 17799:2000, Section 9.7, "Monitoring System Access and Use."	Information Security Booklet (Dec. 2002), pp. 33 & 37.
Policy			
	Establish a firewall policy that addresses, at a minimum: • **Necessary firewall capacities [type of firewall(s) used];** • **Firewall topology and architecture;** • **Permissible traffic*; and** • **Monitoring, testing, and updating.** ***Reason:*** *A firewall policy is a component of the overall security policy and documents how management expects the firewall to function.* *Based on the premise that all traffic is denied unless explicitly permitted.	ISO/IEC 17799:2000, Section 9.4.6, "Segregation in Networks." NSA's "The 60 Minute Network Security Guide", version 1.2, July 2002, p. 10-11	Information Security Booklet (Dec. 2002), pp. 36-37.
Testing			
	Test firewall security regularly, especially after any major network configuration changes. ***Reason:*** *Regular testing of firewall security, especially after changes, ensures that controls are functioning effectively and as intended.*	ISO/IEC 17799:2000, Section 9.4.6, "Segregation in Networks"; Section 8.5.1, "Network Controls"; Section 8.1.3, "Incident Management	Information Security Booklet (Dec. 2002), p. 37. E-Banking Booklet (Aug. 2003), p. 30.

Security

Element		
Essential Practices Statement	**Industry Standard Reference**	**FFIEC IT Examination Handbook Reference**
	Procedures." NSA's "The 60 Minute Network Security Guide", version 1.2, July 2002, p. 10	
Logging		
Activate audit logging, copy logs to a secure file system, and review logs regularly to determine if any unauthorized or unexpected activities have occurred. ***Reason:*** *Appropriate logging controls ensure that security personnel can review and analyze log data to identify unauthorized access attempts and security violations, provide support for personnel actions, and aid in reconstructing compromised systems. Log files often contain sensitive information; therefore, management should strictly control and monitor access. Certain audit logs may be required to be archived as part of a record retention policy or to collect evidence.*	ISO/IEC 17799:2000, Section 9.7.1, "Event Logging."	Information Security Booklet (Dec. 2002), pp. 38, 64-66.
Change Controls		
Establish change control procedures and maintain manual or automatic maintenance records for all program changes. ***Reason:*** *To minimize the corruption of information systems, management must strictly control the implementation of any changes to the firewall and ensure the changes do not compromise the security of either the system or the operating environment.*	ISO/IEC 17799:2000, Section 10.5, "Security in Development and Support Process."	Information Security Booklet (Dec. 2002), pp. 36-38.
Segregation of Duties		
Ensure that logical access controls support segregation of duties. ***Reason:*** *Segregation of duties provides a method for reducing the risk of accidental or deliberate systems misuse. An individual should not be allowed to make and also approve changes to the firewall configuration or logging system. Authorization to make changes should be separate from authorization to approve changes.*	ISO/IEC 17799:2000, Section 8.1.4, "Segregation of Duties."	Information Security Booklet (Dec. 2002), pp. 37-38, 41.

Security

Element	Essential Practices Statement	Industry Standard Reference	FFIEC IT Examination Handbook Reference
5. Event Protection			
	Foundation: Event protection is an essential control against security events, such as network attacks (i.e., denial of service) or the use of malicious code (i.e., viruses, worms, Trojan horses, etc.). Network attacks can prevent legitimate users from accessing the institution's services. Malicious code can perpetrate various attacks from corrupting data to damaging infrastructure. Event protection is also linked to intrusion detection and response. Refer to discussion of intrusion detection systems (IDS) in the ***Operations*** section.	ISO/IEC 17799:2000, Section 8.3, "Protection Against Malicious Software."	Information Security Booklet (Dec. 2002), pp. 53-55.
Controls			
	Train staff about the risks from malicious code. Establish controls to: • **Prohibit the use of untested or unlicensed software;** • **Review the network regularly for unauthorized software;** • **Prohibit the downloading of software from the Internet or personal PCs;** • **Scan all unknown disks, including newly purchased software, before using within the institution's system;** • **Prohibit the use of shareware or freeware that has not been validated; and** • **Promote defensive e-mail practices, such as not opening unexpected messages or those from unknown sources.** ***Reason:*** *Protection efforts involve both security awareness training and preventative controls. An unauthorized user could exploit even a small weakness and cause significant damage to an institution's financial condition, ongoing operations, or reputation.*	ISO/IEC 17799:2000, Section 6.2.1, "Information Security Education and Training"; Section 8.3.1, "Controls Against Malicious Software."	Information Security Booklet (Dec. 2002), pp. 54-55. E-Banking Booklet (Aug. 2003), pp. 29-30.
Anti-virus Software			
	Maintain current anti-virus software (engine) and update virus definition files frequently (at least weekly). ***Reason:*** *Malicious code is created continually and existing code often mutates; therefore, anti-virus products must be updated to protect systems against the latest strains of malicious code.*	ISO/IEC 17799:2000, Section 8.3.1, "Controls Against Malicious Software."	Information Security Booklet (Dec. 2002), pp. 53-55. E-Banking Booklet (Aug. 2003), p. 29.

Security

Element		
Essential Practices Statement	**Industry Standard Reference**	**FFIEC IT Examination Handbook Reference**
Reporting		
Routinely report to the board of directors the type, frequency, severity, and effect of all security events. Additionally, inform the board of the response and recovery actions taken. **Notify the appropriate FCA field office as quickly as possible when institution management suspects a security event that affects ongoing institution operations or other entities (other system institutions, FCA, commercial banks, borrowers, etc.). This would also include situations where the institution activated its disaster recovery or business continuity plan.** ***Reason:*** *The board has a fiduciary responsibility to be aware of threats to the institution and the effectiveness of staff's response and follow-up. This information could show trends and areas of weakness that need further attention.* *Notifying the FCA field office alerts Agency personnel to the existence of an incident, informs them about the institution's response and recovery actions, and enables the Agency to contact other agency officials or legal authorities as necessary.*	FCA Informational Memorandum, "Rescission of Information Systems Bulletin No. 89-2" (April 5, 2000). ISO/IEC 17799:2000, Section 6.3.1, "Reporting Security Incidents."	Information Security Booklet (Dec. 2002), pp. 73-74.